



GVNW CONSULTING, INC.

8050 SW WARM SPRINGS STREET
SUITE 200
P.O. BOX 2330
TUALATIN, OR 97062
TEL 503.612.4400
FAX 503.612.4401
www.gvnw.com

Received & Inspected

FEB 27 2008

FCC Mail Room

February 25, 2008

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
9300 East Hampton Drive
Capitol Heights, MD 20743

DOCKET FILE COPY ORIGINAL


re: EB Docket No. 06-36

Dear Ms. Dortch:

Please find enclosed an original and five (5) copies of the CPNI Compliance Certificate and the Accompanying Statement requirements for St. Paul Telephone Association, TRS #802479.

Please return a stamped copy in the enclosed SASE. If there are any questions, I may be reached on 503-612-4400.

Sincerely,


Carsten Koldsbaek
Consulting Manager

Enclosures

Copies to:
Federal Communications Commission
Enforcement Bureau
445 - 12th Street SW
Washington, DC 20554

Best Copy & Printing Inc.
445 - 12th Street, Suite CY-B402
Washington, DC 20554

No. of Copies rec'd 0+4
List A B C D E



Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Received & Inspected

FEB 27 2008

FCC Mail Room

Annual 64.2009(e) CPNI Certification for 2007

Date filed: February 25, 2008

Name of company covered by this certification: St. Paul Cooperative Telephone Association

Form 499 Filer ID: 802479

Name of signatory: Nick L. Schneider

Title of signatory: Secretary Treasurer

I, Nick L. Schneider certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any action against data brokers in the past year. To the best of our knowledge, no pretexters have attempted to access CPNI at our company.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed Nick L. Schneider

Nick L. Schneider



February 25, 2008

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Reference: EB Docket No. 06-36; Annual CPNI Certification Filing of St. Paul Cooperative Telephone Association

Dear Ms. Dortch:

Enclosed is the 2007 CPNI Certification filing of St. Paul Cooperative Telephone Association (St. Paul) (TRS # 802479) in response to the Commission's April 2, 2007 order in CC Docket No. 96-115 and WC Docket No. 04-36. This certification is required by section 64.2009(e) of the Commission's rules.

During the year 2007, St. Paul did not detect any data broker activity regarding the CPNI of any customer of St. Paul. As a result, St. Paul did not undertake any legal or regulatory actions against data brokers.

The enclosed Procedures and Policies manual of St. Paul provides guidance to the employees of St. Paul for protecting the confidentiality of CPNI. This manual also includes the disciplinary procedures applicable to the improper disclosure of CPNI, the processes used to ensure that the opt-out elections are recorded and followed and other measures relevant to demonstrating compliance with the CPNI rules. All employees of St. Paul, who have access to CPNI, were provided training in the use of the manual during 2007. St. Paul takes very seriously its responsibilities in protecting the CPNI of its customers.

St. Paul does not have any new information to report to the Commission regarding the processes that pretexters use to attempt to access the CPNI of customers.

There were no customer complaints concerning the unauthorized release of CPNI recorded for the year 2007.

There were no security issues or customer complaints at St. Paul that would be cause for providing a redacted version of this filing.

Please contact me with any questions or concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "Nick L. Schneider", with a stylized flourish at the end.

Nick L. Schneider
Secretary Treasurer

enclosures

cc: Byron McCoy, byron.mccoy@fcc.gov
Best Copy and Printing, Inc. (BCPI), fcc@bcpiweb.com



CPNI

POLICIES & PROCEDURES MANUAL

Approved by:

General Manager

Date

Effective: _____

TABLE OF CONTENTS

| | |
|---|----|
| <i>Definitions</i> | 3 |
| <i>Company Policy regarding CPNI</i> | 6 |
| <i>Marketing Programs</i> | 6 |
| <i>Release of Call Detail Information</i> | 7 |
| <i>Annual Certification</i> | 8 |
| <i>Notice of Unauthorized Disclosure of CPNI</i> | 8 |
| <i>Safeguards by St. Paul</i> | 10 |
| <i>Training of Employees</i> | 11 |
| <i>Annual Review by Company Management</i> | 12 |
| <i>Forms</i> | |
| <i>Form 1 – Employee Training Certification</i> | 13 |
| <i>Form 2 – Certification of CPNI Filing</i> | 14 |
| <i>Form 3 – Breach Notification – Law Enforcement</i> | 15 |
| <i>Form 4 – Breach Notification – Customer</i> | 16 |
| <i>Form 5 – Notification of Account Changes</i> | 17 |
| <i>Form 6 – Certification of Marketing Campaign Effort</i> | 18 |
| <i>Form 7-W – CPNI Customer Notification (with password)</i> | 19 |
| <i>Form 8-W – Annual CPNI Notice (with password & opt out)</i> | 22 |
| <i>Form 9 – Record of Customer Complaints Concerning</i> <i>the Unauthorized Release of CPNI</i> | 24 |
| <i>Form 10 – Notice of Failure of Opt-out Mechanism</i> | 25 |

Definitions

This St. Paul Cooperative Telephone Association (hereinafter St. Paul) CPNI policy manual relies on the following definitions:

- (1) **Account information.** "Account information" is information that is specifically connected to the customer's service relationship with St. Paul, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.
- (2) **Address of record.** An "address of record," whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.
- (3) **Affiliate.** The term "affiliate" means a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another to own an equity interest (or the equivalent thereof) of more than 10 percent.
- (4) **Breach.** When a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.
- (5) **Call detail information.** Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.
- (6) **Communications-related services.** The term "communications-related services" means telecommunication services, information services typically provided by St. Paul and services related to the provision or maintenance of customer premises equipment.
- (7) **Customer.** A customer of St. Paul is a person or entity to which St. Paul is currently providing service.
- (8) **Customer premises equipment (CPE).** The term "customer premises equipment (CPE)" means equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications.
- (9) **Customer Proprietary Network Information.** The term "customer proprietary network information" means –
 - (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of St. Paul, and that is made available to St. Paul solely by virtue of the St. Paul-customer relationship; and
 - (B) information contained in the bill pertaining to telephone exchange service or telephone toll service received by a customer of St. Paul; except that such term does not include subscriber list information.
- (10) **Data broker.** A person or business that offers for sale CPNI obtained by pretexting.

- (11) **Data bureau.** A company that provides information technology services to telecommunications carriers, specifically billing services and customer record detail. Data bureaus typically have access to call detail CPNI (see Independent contractor).
- (12) **FCC.** The acronym "FCC" refers to the Federal Communications Commission.
- (13) **Independent contractor.** Any person or business that may provide services to telecommunications carriers. This includes, but is not limited to; joint venture partners and independent contractors for the purposes of marketing communications-related services to a customer; billing services; customer record detail; central office equipment vendors; engineering; and construction. Independent contractors typically have access to call detail and/or non-call detail CPNI.
- (14) **Information services typically provided by St. Paul.** The phrase "information services typically provided by St. Paul" means only those information services that are typically provided by St. Paul, such as Internet access or voice mail services. Such phrase "information services typically provided by St. Paul," as used in this manual, shall not include retail consumer services provided using Internet website (such as travel reservation services or mortgage lending services), whether or not such services may other wise be considered to be information services.
- (15) **Joint venture partners** (short term alliances of telecommunications carriers) **and independent contractors** (see Independent contractors) **for the purposes of marketing communications-related services to a customer.** A specific subset of persons or businesses that provide marketing services to telecommunications carriers. Any marketing use of CPNI by this subset must have opt-in approval by the affected customers.
- (16) **Local exchange carrier (LEC).** The term "local exchange carrier (LEC)" means any person that is engaged in the provision of telephone exchange service or exchange access. Such term does not include a person insofar as such person is engaged in the provision of a commercial mobile service under section 332(c) of TA-96, except to the extent that the Commission finds that such service should be included in the definition of such term.
- (17) **Opt-in approval.** The term "opt-in approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that St. Paul obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the St. Paul's request consistent with the requirements.
- (18) **Opt-out approval.** The term "opt-out approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the waiting period described after the customer is provided appropriate notification of St. Paul's request for opt-out consent consistent with the rules.

- (19) **Password.** The term "password" means a secret word or sequence of alpha and numeric characters which is used to limit access to a customer's account to authorized individuals.
- (20) **Pretexting.** The term "pretexting" means the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records.
- (21) **Readily available biographical information.** "Readily available biographical information" is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.
- (22) **Subscriber list information (SLI).** The term "subscriber list information" means any information –
(A) identifying the listed names of subscribers of St. Paul and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and
(B) St. Paul or an affiliate has published, caused to be published, or accepted for publication in any directory format.
- (23) **St. Paul or carrier.** The terms "St. Paul Cooperative Telephone Association," "St. Paul," or "carrier" shall have the same meaning.
- (24) **Telecommunications service.** The term "telecommunications service" means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.
- (25) **Telephone number of record.** The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."
- (26) **Valid photo identification.** The term "valid photo identification" means an official identification document issued by a federal or state governmental agency that identifies the holder of the document that includes a photograph of sufficient clarity to positively identify the holder of the document.

Company Policy Regarding CPNI

St. Paul may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, long distance, and CMRS (wireless)) to which the customer already subscribes from St. Paul, without customer approval. St. Paul does not provide wireless service.

St. Paul has chosen not to use CPNI data that enables the company or its affiliates to market additional products or services. Accordingly, St. Paul's personnel are trained not to use CPNI for such purposes. Because CPNI is not used for marketing purposes, St. Paul has established the appropriate safeguards for this type of treatment (non-use) of CPNI data. These safeguards include documentation of this policy in this manual and training of St. Paul personnel with regard to non-use of CPNI data.

If St. Paul should revise its policies regarding use of CPNI for marketing, it has developed a procedure (Form 10) to notify the FCC in writing within five days of any instance when its opt-out policies do not work properly, to such a degree that the customer's inability to opt-out is more than an anomaly.

In this effort, the Company must follow all applicable FCC rules as contained in Subpart U – Customer Proprietary Network Information – of Part 64 of Title 47 of the Code of Federal Regulations. Specific St. Paul procedures are as follows:

BUSINESS CUSTOMER EXEMPTION

St. Paul has no business customers that would qualify for the business customer exemption.

ACCESS TO CPNI DATA

Access to CPNI data is limited to employees or entities with the requisite proper authorization as allowed by FCC rules. Any employees or entities with CPNI access must operate under policies that require nondisclosure of confidential information. Improper use or disclosure of CPNI by employees is subject to disciplinary action up to and including termination.

Marketing Programs

No St. Paul marketing campaigns are related to CPNI. As a logical outcome of this policy, St. Paul uses neither opt-in nor opt-out approval from customers with regard to any marketing.

Contact the General Manager if you are uncertain as to the type of information you can use in marketing services to customers.

CUSTOMER NOTICE AT INITIATION OF SERVICE

Customers are informed during the initiation of service with St. Paul that their CPNI data is not used for marketing purposes. Customers receive annual reminders (Form 8-W) of this CPNI policy.

CUSTOMER NOTICE

Adequate notice with respect to customer CPNI rights and St. Paul's duty to protect CPNI is provided in St. Paul's telephone directory. In addition, a CPNI notice is printed periodically on the customer's billing statement.

RECORD OF CUSTOMER COMPLAINTS CONCERNING THE UNAUTHORIZED RELEASE OF CPNI

All customer complaints concerning the unauthorized release of CPNI will be logged (Form 9) and retained for a period of five years. This information is summarized and included with St. Paul's annual certification to the FCC.

Release of Call Detail Information (Forms 7-W & 8-W)

CUSTOMER INITIATED TELEPHONE ACCOUNT ACCESS

Release of any CPNI information requested by the customer via a telephone call is prohibited except when:

- the requesting individual provides the password of record; or
- the information will be sent via USPS mail to the customer's address of record; or
- St. Paul will call the telephone number of record and disclose the call detail information.

If the customer has forgotten their password or does not have a password established, St. Paul can proceed with routine customer care procedures if the customer can provide all of the call detail information. St. Paul will not disclose any call detail other than the information the customer disclosed during that particular contact.

RETAIL LOCATION ACCOUNT ACCESS

Customers or their authorized contacts as allowed by the Telecommunications Act of 1996 – Section 222(c)(2) must have a valid, government issued photo identification, such as a driver's license, passport, or comparable ID to obtain CPNI information.

ON-LINE ACCOUNT ACCESS

St. Paul does not have on-line account access for its customers.

NOTIFICATION OF ACCOUNT CHANGES

St. Paul will notify (Form 5) any customer immediately of any account changes including password, customer response to company designed back-up means of authentication, on-line account, address of record, and any other record that may be created or changed. This notification will be through a voicemail or by USPS mail to the address of record as it was prior to the change.

New customers are exempt from this notification at service initiation.

PROCEDURES TO PROTECT AGAINST PRETEXTING

Pretexting is the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications record. The Company has employed the above procedures and safeguards in order to achieve reasonable measures designed to discover and protect against pretexting.

Annual Certification

St. Paul will certify annually (Form 2) compliance to the CPNI rules. This certification will be filed with the FCC and will be made publicly available by request.

St. Paul's annual certification will be signed by an officer as an agent of St. Paul, stating that he/she has personal knowledge the company has established operating procedures that are adequate to comply with the FCC CPNI rules.

In addition to the annual certification, St. Paul will provide an accompanying statement explaining how the company's procedures ensure the company is or is not in compliance with the FCC's CPNI rules. In the explanation, St. Paul will include:

- the training employees receive to protect CPNI.
- the disciplinary process applicable to improper disclosure of CPNI.
- other measures relevant to demonstrate compliance with the FCC's CPNI rules.

Notice of Unauthorized Disclosure of CPNI

St. Paul is required by FCC rules to notify law enforcement of any CPNI breaches no later than seven (7) days after a reasonable determination of a breach has occurred. St. Paul will send an electronic notification through the central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). This notification will include a description of the CPNI that was disclosed, how the breach was discovered, an analysis of the sensitivity of the breached CPNI, and any corrective measures taken to prevent recurrence of such breach.

Responsibility to notify USSS and FBI has been assigned to the General Manager.

NOTIFICATION OF CPNI SECURITY BREACHES

- (1) *Notification of law enforcement agencies* (Form 3). St. Paul will notify law enforcement of a breach of its customers' CPNI as stated in this section of St. Paul's CPNI manual. St. Paul will not notify any of its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement as required and spelled out below.

- (2) *Limitations.* As soon as practicable, but in no event later than seven (7) business day, after reasonable determination of the breach, St. Paul shall electronically notify the **United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI)** through a central reporting facility. This will be done through the FCC's link to the reporting facility at <http://www.fcc.gov/eb/cpni>.

- a) Notwithstanding any state law to the contrary, St. Paul shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as in the following two parts of this section.
- b) If St. Paul believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under the above paragraph of this section, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. St. Paul shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.
- c) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct St. Paul not to disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify St. Paul when it appears the public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to St. Paul, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writing shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

- (3) *Customer Notification* (Form 4). After St. Paul has completed the process of notifying law enforcement as listed above, it shall notify its customers of a breach of those customers' CPNI.

- (4) *Recordkeeping.* St. Paul will maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI as defined in the above section of this manual, and all notifications made to customers. This record must include, if available:

- a) Dates of discovery and notification.
- b) A detailed description of the CPNI that was the subject of the breach.
- c) The circumstances of the breach.
- d) St. Paul will retain the record for a minimum of 2 years.

- (5) *Supersede.* This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is

inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

SAFEGUARDS BY ST. PAUL

CUSTOMER RECORDS

Customer service records will clearly establish customer CPNI approval. Record of this approval will be kept for a minimum of one year. The record is designed by St. Paul's service bureau Mid America Computer Corporation (MACC).

All personnel of St. Paul will be trained annually or upon commencement of employment regarding CPNI policies. These policies include when the employee is authorized to use and when they are NOT authorized to use CPNI. Any infractions of St. Paul's CPNI policies will be reported to the General Manager and a record will be made of the infraction(s) and the disciplinary steps taken.

Discipline for infractions of the policies will be in the form of a letter of reprimand to the employee's file for an initial infraction, two days off without pay for a second infraction, five days off without pay for a third infraction, and termination in the case of a fourth infraction within a twelve month period.

INTERFACE WITH CALEA COMPLIANCE

In order to comply with certain Communications Assistance for Law Enforcement Agencies (CALEA) rules, St. Paul has engaged the services of Intelleg, a trusted third party provider. This third party provider is involved in the event of a request for certain types of surveillance activities by Law Enforcement Agencies (LEAs).

St. Paul has added the following addendum to its third party provider CALEA contract:

"Whereas St. Paul is required by law and its company policies to protect the privacy and security of the information regarding its customers,

To the extent that Intelleg, in rendering services for St. Paul receives customer proprietary network information, as that term is defined under 47 U.S.C. Section 222 and interpreted by the FCC ("CPNI"), Intelleg shall maintain the confidentiality of such CPNI according to the policies and procedures implemented by St. Paul. Intelleg shall promptly delete from its records any CPNI that is received by Intelleg which is not delivered to an LEA pursuant to a lawfully authorized intercept request."

INTERFACE WITH CONTRACTORS

St. Paul has occasion to utilize contractors for specific projects needed to conduct its business. St. Paul requires all its contractors to include the following language in all agreements with St. Paul:

"Whereas St. Paul is required by law and its company policies to protect the privacy and security of the information regarding its customers,

To the extent that [Name of Contractor], in rendering services for St. Paul receives customer proprietary network information, as that term is defined under 47 U.S.C. Section 222 and interpreted by the FCC ("CPNI"), [Name of Contractor] shall maintain the confidentiality of *such CPNI according to the policies and procedures implemented by St. Paul.* [Name of Contractor] shall promptly delete from its records any CPNI that is received by [Name of Contractor] in its engagement with St. Paul."

TRAINING OF EMPLOYEES

EMPLOYEE TRAINING

The company provides training to employees on the proper use and disclosure of CPNI.

Emphasis on the company policy that no customer will be subject to marketing based on CPNI data is included as a part of the employee training.

St. Paul specific CPNI training will be provided annually and with each newly hired employee. Documentation of training (Form 1) will be kept on file for a period of at least five years.

ANNUAL REVIEW BY COMPANY MANAGEMENT

St. Paul treats customer privacy as a serious issue. St. Paul is proud of its long history of reliable, trustworthy service and is vigilant in the steps that will be taken to ensure customer privacy. Accordingly, St. Paul policy requires this CPNI Policy Manual to be reviewed on an annual basis. This review is conducted at a time set by the General Manager each calendar year. The General Manager's annual review will include, but may not be limited to a review with GVNW Consulting, Inc.